Amendments to the Claims

This listing of claims will replace all prior version, and listings, of claims in the application:

Listing of Claims

1. (Currently amended) A network security system for permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

a port monitoring unit for extracting information about a server port being used ~~through~~ by a network communication program;

an internal permitted program storage for extracting information about a program for which communication is permitted by the firewall[[~~,~~]] and registering the extracted information;

an internal permitted port storage[[~~,~~]] registering the extracted information about the server port if the ~~port monitoring unit extracts~~ network communication program extracted from the information about the server port ~~being used using the program~~ is registered in the internal permitted program storage~~, registering the extracted information about the server port~~; and

a ~~device for making the~~ firewall flexible device~~,~~ determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage[[~~,~~]] and blocking the packet of inbound traffic if the destination port has not been registered~~, transmitting the corresponding packet to the firewall, and if the destination port has been registered, allowing the corresponding packet to bypass the firewall~~.

2. (Currently amended) The network security system as set forth in claim 1, wherein the information about the program, which is extracted and registered in the internal permitted program storage, includes information about at least one of a program name, an entire path of the program, and a program ~~Message Digest 5 (MD5)~~ hash value.

3. (Currently amended) The network security system as set forth in claim 1, wherein the information about the server port, which is ~~extracted and~~ registered in the internal permitted port storage, includes information about at least one of an entire path of the program, a protocol, and a port.

4. (Currently amended) A network security method of permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

~~the first step of~~ extracting information about a server port being used ~~through~~ by a network communication program;

~~the second step of~~ extracting information about a program for which communication is permitted by the firewall[[~~,~~]] and registering the extracted information in an internal permitted program storage;

~~the third step of,~~ registering the information about the extracted server port in an internal permitted port storage if the network communication program extracted from the information about the server port ~~being used~~ is ~~extracted using the program~~ registered in the internal permitted program storage ~~at the first step, registering the information about the extracted server port in internal permitted port storage~~;

~~the fourth step of~~ determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage; and

~~the fifth step of, if, as a result of the determination at the fourth step,~~ blocking the packet of inbound traffic if the destination port has not been registered~~, transmitting the packet of inbound traffic to the firewall; and~~

~~the sixth step of, if, as a result of the determination at the fourth step, the destination port has been registered, allowing the corresponding packet to bypass the firewall~~.

5. (Canceled)

6. (Canceled)

7. (Canceled)

8. (Currently amended) The network security method as set forth in claim 4, wherein the information about the program~~, which is extracted and registered at the second step,~~ includes information about at least one of a program name, an entire path of the program, and a program ~~Message Digest 5 (MD5)~~ hash value.

9. (Currently amended) The network security method as set forth in claim 4, wherein the information of the server port~~, which is extracted and registered at the third step,~~ includes information about at least one of an entire path of the program, a protocol, and a port.

10. (Currently amended) A computer-readable recording medium for performing a network security method using a

firewall, the medium storing a program for executing the method, the method comprising:

~~the first step of~~ extracting information about a server port being used ~~through~~ by a network communication program;

~~the second step of~~ extracting information about a program for which communication is permitted by the firewall[[~~,~~]] and registering the extracted information in an internal permitted program storage;

~~the third step of,~~ registering the information about the extracted server port in an internal permitted port storage if the network communication program extracted from the information about the server port ~~being used~~ is ~~extracted using the program~~ registered in the internal permitted program storage ~~at the first step, registering the information about the extracted server port in internal permitted port storage~~;

~~the fourth step of~~ determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage; and

~~the fifth step of, if, as a result of the determination at the fourth step,~~ blocking the packet of inbound traffic if the destination port has not been registered~~, transmitting the packet of inbound traffic to the firewall; and~~

~~the sixth step of, if, as a result of the determination at the fourth step, the destination port has been registered, allowing the corresponding packet to bypass the firewall~~.

11. (New) The network security system as set forth in claim 1, wherein the firewall flexible device allows the packet of inbound traffic to bypass the firewall if the destination port been registered.

12. (New) The network security method as set forth in claim 4, further comprising:

allowing the packet of inbound traffic to bypass the firewall if the destination port has been registered.